M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
Brandon P. Jack (SBN 325584)
Michelle Zhu (SBN 347741)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
12100 Wilshire Boulevard, Suite 800
Los Angeles, CA 90025
Tel: (747) 777-7748
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com
mzhu@justice4you.com

Attorneys for Plaintiff and the Proposed Class

IN THE UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

SAMUEL TSOU, on behalf of himself and all others similarly situated,

Plaintiff,

v.

CITY OF HOPE NATIONAL MEDICAL CENTER d/b/a CITY OF HOPE,

Defendant.

Case No. _____

CLASS ACTION

DEMAND FOR A JURY TRIAL

Plaintiff Samuel Tsou ("Plaintiff") brings this Class Action Complaint ("Complaint") against City of Hope National Medical Center d/b/a City of Hope ("Hope" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

SUMMARY OF ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive information of its patients.

2. Defendant is a cancer research, treatment, and prevention organization that provides healthcare services for "patients across the United States through [its] national footprint of cancer centers."[1]

3. Plaintiff's and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was targeted, compromised, and unlawfully accessed due to the Data Breach.

4. Defendant collected and maintained certain personally identifiable information ("PII") and protected health information ("PHI") of Plaintiff and the putative Class Members (defined below), who are current and former patients at Defendant.

5. Specifically, the sensitive information compromised in the Data Breach included Plaintiff's and Class Members' PII and PHI such as their full names, email addresses, phone numbers, dates of birth, Social Security numbers, driver's license or other government identification, financial details including bank account numbers and/or credit card details, health insurance information, medical records and information about medical history and/or associated conditions, and/or unique identifiers to associate individuals with City of Hope (e.g. medical record numbers).

[1] *See* https://www.cityofhope.org/ (last visited April 17, 2024).

("PHI" and "PII" shall be collectively referred to herein as "Private Information".)

6. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

7. As a result of the Data Breach, Plaintiff and approximately 827,149 Class Members,[2] suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's and Class Members' Private Information being disseminated on the dark web; (ix) a significant decrease in Plaintiff's credit score; (x) statutory damages; (xi) nominal damages; and (xii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patients' Private Information from a foreseeable and preventable cyber-attack.

9. Moreover, upon information and belief, Defendant was targeted for a cyber-attack due to its status as a healthcare entity that collects and maintains highly valuable Private Information on its systems.

[2] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/e86f6a2d-d729-49a3-83b0-f9c46afa5b9b.shtml (last visited on April 17, 2024).

10. Defendant maintained, used, and shared the Private Information in a reckless manner. In particular, the Private Information was used and transmitted by Defendant in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

11. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

12. Plaintiff's and Class Members' identities are now at risk due to Defendant's negligent conduct because the Private Information that Defendant collected and maintained has been accessed and acquired by data thieves.

13. Armed with the Private Information accessed in the Data Breach, cyber-thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

15. Plaintiff and Class Members may also incur out-of-pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

18. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.[3]

20. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

[3] According to the breach report submitted to the Office of the Maine Attorney General, 166 Maine residents were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/1bb296e2-ea79-438c-b357-28ef738a0bf6.shtml (last visited on April 17, 2024).

21. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

PARTIES

22. Plaintiff Samuel Tsou is a resident and citizen of El Monte, California.

23. Defendant Hope is a corporation organized under the state laws of California with its principal place of business located in Duarte, California.

FACTUAL ALLEGATIONS

Defendant's Business

24. As a National Cancer Institute (NCI)-designated comprehensive cancer center for cancer research, prevention, and treatment, Defendant provides healthcare services for "patients across the United States through [its] national footprint of cancer centers."[4]

25. Plaintiff and Class Members are current and former patients of Defendant.

26. In the course of their relationship, patients, including Plaintiff and Class Members, provided Defendant with at least the following Private Information: names, dates of birth, contact information, health insurance information, Social Security numbers, and other sensitive information.

27. Upon information and belief, in the course of collecting Private Information from patients, including Plaintiff, Defendant promised to provide confidentiality and adequate security for the data it collected from patients through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

28. Indeed, Defendant provides on its website that: "[w]e are required by law to maintain the privacy of your protected health information ("PHI"), to provide you

[4] *See* https://www.cityofhope.org/ (last visited on April 17, 2024).

with notice of our legal duties and privacy practices with respect to your PHI, and to notify you in the event of a breach of your unsecured PHI."[5]

29. Plaintiff and the Class Members, as patients at Defendant, relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Patients, in general, demand security to safeguard their Private Information, especially when their Social Security numbers and other sensitive Private Information are involved.

The Data Breach

30. On or about April 2, 2024, Defendant began sending Plaintiff and other Data Breach victims a Notice of Data Breach letter (the "Notice Letter"), informing them that:

> ***What Happened?***
>
> On or about October 13, 2023, City of Hope became aware of suspicious activity on a subset of its systems and immediately instituted mitigation measures to minimize any disruption to its operations. City of Hope launched an investigation into the nature and scope of the incident with the assistance of a leading cybersecurity firm, which determined that an unauthorized third party accessed a subset of our systems and obtained copies of some files between September 19, 2023, and October 12, 2023. City of Hope has undertaken a detailed review of the copied files to determine the incident's impact and has determined that some of these files may have contained your information.
>
> ***What Information Is Involved?***
>
> While the investigation remains ongoing, the impacted personal information identified thus far varies by individual but may have included name, contact information (e.g., email address, phone number), date of birth, social security number, driver's license or other government

[5] *See* https://www.cityofhope.org/sites/www/files/2024-03/COH-Notice-of-Privacy-Practices-09-2023_ English.pdf (last visited on April 17, 2024).

> identification, financial details (e.g., bank account number and/or credit card details), health insurance information, medical records and information about medical history and/or associated conditions, and/ or unique identifiers to associate individuals with City of Hope (e.g., medical record number).[6]

31. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

32. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of critical facts regarding the Data Breach. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

33. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be inferred from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted information including Plaintiff's and Class Members' Social Security numbers, PHI, and other sensitive information for viewing, download, and exfiltration or theft.

34. In the context of notice of data breach letters of this type, Defendant's use of the phrase "may have contained" is misleading. Companies only send notice letters because data breach notification laws require them to do so. Such letters are only sent

---

[6] *See* the "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/1bb296e2-ea79-438c-b357-28ef738a0bf6.shtml (last visited on April 17, 2024).

to those persons whom Defendant itself has a reasonable belief that personally identifiable and/or protected health information was accessed or acquired by an unauthorized individual or entity. Indeed, by sending a notice of data breach letter to Plaintiff and Class Members, Defendant admits that it has a reasonable belief that Plaintiff's and Class Members' Private Information was accessed or acquired by cybercriminals.

35. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook any efforts to contact the approximate 827,149 Class Members whose data was accessed and acquired in the Data Breach.

36. Defendant had obligations created by the FTC Act, HIPAA, contract, common law, and industry standards to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

37. Despite these obligations, Defendant did not implement or use any reasonable or appropriate security procedures and practices - such as encrypting the Private Information or deleting it when it is no longer needed - to protect Plaintiff and Class Member's Private Information thereby causing the exposure of their Private Information.

38. As such, the attacker was able to access and acquire files Defendant kept and maintained containing the unencrypted Private Information of Plaintiff and Class Members. This resulted in Plaintiff's and Class Members' Private Information being accessed and stolen in the Data Breach.

39. Plaintiff reasonably believes that the compromised Private Information of the Class was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

40. Defendant did not implement or use any reasonable or appropriate security procedures and practices - such as encrypting the Private Information or

deleting it when it is no longer needed - to protect Plaintiff and Class Member's Private Information thereby causing the exposure of their Private Information.

41. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

42. As the Federal Bureau of Investigation explains, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[7]

43. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

[7] *See How to Protect Your Networks from RANSOMWARE*, at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited on April 17, 2024).

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalApp Data folder.

- Consider disabling the Remote Desktop Protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[8]

44. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates

[8] *Id.* at 3-4.

- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply the principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[9]

[9] *See Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited on April 17, 2024).

45. Given that Defendant was storing the Private Information of its current and former patients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

46. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and cybercriminals acquiring and accessing the Private Information of more than eight hundred thousand individuals, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, And Stores Its Patients' Private Information

47. Defendant acquires, collects, and stores a massive amount of Private Information on its current and former patients.

48. As a condition of obtaining healthcare services at Defendant, Defendant requires that patients and other personnel entrust it with highly sensitive personal information.

49. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

50. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. They would not have entrusted it to Defendant absent a promise to safeguard that information.

51. Upon information and belief, in the course of collecting Private Information from patients, including Plaintiff, Defendant promised to provide confidentiality and adequate security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

52. Indeed, Defendant provides on its website that: "[w]e are required by law to maintain the privacy of your protected health information ("PHI"), to provide you

with notice of our legal duties and privacy practices with respect to your PHI, and to notify you in the event of a breach of your unsecured PHI."[10]

53. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew, Or Should Have Known, of the Risk Because Healthcare Entities In Possession Of Private Information Are Particularly Susceptible To Cyber Attacks

54. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendant, preceding the date of the breach.

55. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

56. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[11]

57. In light of recent high-profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

---

[10] *See* https://www.cityofhope.org/sites/www/files/2024-03/COH-Notice-of-Privacy-Practices-09-2023_English.pdf (last visited on April 17, 2024)

[11] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last visited on April 17, 2024)

58. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are often attractive to ransomware criminals because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[12]

59. Additionally, as companies became more dependent on computer systems to run their business,[13] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[14]

60. Defendant knew and understood unprotected or exposed Private Information in the custody of insurance companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

61. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

---

[12] *See* John Sakellariadis, *Behind the rise of ransomware*, https://www.atlantic council.org/in-depth-research-reports/issue-brief/behind-the-rise-of-ransomware/ (last visited on April 17, 2024).

[13] *See Implications of Cyber Risk for Financial Stability*, https://www.federalreserve .gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220 512.html (last visited on April 17, 2024).

[14] *See Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited on April 17, 2024).

62. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

63. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

64. The ramifications of Defendant's failure to secure the Private Information of Plaintiff and Class Members are long-lasting and severe. Once Private Information is stolen—particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

65. In the Notice Letter, Defendant offers 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

66. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and Class Members' sensitive Private Information was, in fact, affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

67. As a healthcare entity in custody of the Private Information of its patients, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Private Information

68. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

69. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[17]

70. For example, Personal Information can be sold at a price ranging from $40 to $200.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

71. Moreover, Social Security numbers are among the worst kinds of Private Information to have stolen because they may be used for a variety of fraudulent purposes and are difficult for an individual to change.

---

[15] 17 C.F.R. § 248.201 (2013).

[16] *Id.*

[17] *See Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on April 17, 2024).

[18] *See Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on April 17, 2024).

[19] *See In the Dark*, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited on April 17, 2024).

72. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [20] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[21]

73. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[22]

74. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[23] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[24]

---

[20] *See Avoid Identity Theft: Protect Social Security Numbers*, https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases (last visited on April 17, 2024).

[21] *Id.*

[22] *See* Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited on April 17, 2024).

[23] *See How to Protect Yourself from Social Security Number Identity Theft,* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last visited on April 17, 2024).

[24] *See What is an SSN? Facts to Know About Social Security Numbers*, https://www.investopedia.com/terms/s/ssn.asp (last visited on April 17, 2024).

75. What's more, changing or canceling a stolen Social Security number is no easy task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

76. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[25]

77. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiffs' Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the

[25] *See* Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited on April 17, 2024).

victim] and target her in fraudulent schemes and identity theft attacks.").

78. Similarly, the California state government warns patients that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[26]

79. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[27]

80. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[28]

81. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

---

[26] *See Your Social Security Number: Controlling the Key to Identity Theft*, https://oag.ca.gov/idtheft/facts/your-ssn (last visited on April 17, 2024).

[27] *See Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658 (last visited on April 17, 2024).

[28] *Id*.

82. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[29] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[30]

83. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[31]

84. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[32]

85. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information

---

[29] *See* Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited on April 17, 2024).

[30] *Id.*

[31] *See How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited on April 17, 2024).

[32] *See Medical I.D. Theft*, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last visited on April 17, 2024).

(*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

86. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[33] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[34] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30 percent of overall health data breaches.[35]

87. Reportedly, medical data sells for $50 and up on the Dark Web.[36]

88. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse

---

[33] *See* Adil Hussain Seh et al, *Healthcare Data Breaches: Insights and Implications*, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last visited on April 17, 2024).

[34] *See* Steve Elder, *December 2019 Healthcare Data Breach Report*, https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last visited on April 17, 2024).

[35] *See* Samatha Schwartz, *55% of healthcare breaches feature ransomware: report* https://www.cybersecuritydive.com/news/ransomware-data-breach-healthcare-cost-tenable/596451/#:~:text=Healthcare%20systems%20are%20the%20most%20compromised%20segment%20of,%285%25%29%20and%20government%20agencies%20%284%25%29%2C%20according%20to%20Tenable (last visited on April 17, 2024).

[36] *See Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://news.sophos.com/en-us/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/ (last visited on April 17, 2024).

yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[37]

89. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[38] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[39]

90. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers, PHI, dates of birth, and names.

91. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[40]

---

[37] *See* Michael Ollove, *The Rise of Medical Identity Theft in Healthcare* (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ (last visited on April 17, 2024).

[38] *See* Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited on April 17, 2024).

[39] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited on April 17, 2024).

[40] *See* Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen*

92. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

93. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[41]

94. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Defendant Fails To Comply With FTC Guidelines

95. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

Credit Card Numbers, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited on April 17, 2024).

[41] *See Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited on April 17, 2024).

96. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[42]

97. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[43]

98. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

99. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[42] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on April 17, 2024).

[43] *Id.*

100. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (Henry Ford) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

101. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

102. Defendant failed to properly implement basic data security practices.

103. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information of its patients or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

104. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its patients; Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Fails To Comply With HIPAA Guidelines

105. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102). It is required to comply with HIPAA Privacy Rule and Security Rule, 45 C.F.R. Parts 160 and 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Parts 160 and 164, Subparts A and C.

106. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[44] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

107. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

108. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

109. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

110. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

111. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

112. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and

[44] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

113. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

114. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[45]

115. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

116. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

117. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance

[45] *See* Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[46] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[47]

Defendant Fails To Comply With Industry Standards

118. As noted above, experts studying cyber security routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

119. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

---

[46] *See* http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited on April 17, 2024).

[47] *See* https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited on April 17, 2024).

120. Other best cybersecurity practices that are standard for healthcare entities include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

121. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

122. These foregoing frameworks are existing and applicable industry standards for healthcare entities, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries & Damages

123. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data

Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

Data Breaches Increase Victims' Risk Of Identity Theft

124. As Plaintiff has already experienced, the unencrypted Private Information of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

125. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

126. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

127. Plaintiff's and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

128. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause

great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[48]

129. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective patients."[49]

130. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a patient's identity after the initial account setup[.]"[50] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account."[51]

131. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[52]

---

[48] *See* N.C. Gen. Stat. § 132-1.10(1).

[49] *See* Husayn Kassal, *Banks need to stop relying on Social Security numbers* (November 12, 2018), https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers (last visited on April 17, 2024).

[50] *See* Ann Carrns, *Just 5 Banks Prohibit Use of Social Security Numbers*, https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/ (last visited on April 17, 2024).

[51] *See* What Can Someone Do With Your Social Security Number?, https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited on April 17, 2024).

[52] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on

132. With "Fullz" packages, cybercriminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

133. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

134. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like insurance information) of Plaintiff and the other Class Members.

135. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

---

a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited on April 17, 2024).

136. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

137. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time have been lost.

138. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiff and Class Members to take the following measures to protect themselves: "[w]e encourage you to remain vigilant to protect against potential fraud and identity theft by reviewing your account statements, monitoring your credit reports, and notifying your financial institutions of any potential suspicious activity."[53]

139. In addition, Defendant's Notice letter includes a full two pages devoted to "Steps You Can Take To Help Protect Your Information" that recommend Plaintiff and Class Members to partake in activities such as enrolling in the credit monitoring services offered by Defendant, obtaining credit reports, and contacting government agencies.[54]

140. Defendant's extensive suggestion of steps that Plaintiff and Class Members must take in order to protect themselves from identity theft and/or fraud

---

[53] *See "ME Notice Attachment Letter.pdf*" available at https://apps.web.maine.gov/online/aeviewer/ME/40/1bb296e2-ea79-438c-b357-28ef738a0bf6.shtml (last visited April 18, 2024).

[54] *Id.*

demonstrates the significant time that Plaintiff and Class Members must undertake in response to the Data Breach. Plaintiff's and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiff and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Defendant's Notice Letter.

141. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, signing up for credit monitoring and identity theft protection services, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect. Accordingly, the Data Breach has caused Plaintiff and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

142. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[55]

143. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[56]

---

[55] *See* United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited on April 17, 2024).

[56] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited on April 17, 2024).

144. For those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[57]

Diminution of Value of Private Information

145. PII and PHI are valuable property rights.[58] Their inherent value is clear given the significant importance of Big Data in corporate America and the severe penalties, such as heavy prison sentences, that follow cyber thefts. This straightforward risk-to-reward analysis further confirms without a doubt that Private Information holds considerable market value.

146. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[59]

147. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[60]

---

[57] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report") (last visited on April 17, 2024).

[58] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[59] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited on April 17, 2024).

[60] *See* David Lazarus, *Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited on April 17, 2024).

148. In fact, the data marketplace is so sophisticated that patients can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[61]

149. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[62]

150. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[63]

151. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

152. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

---

[61] https://datacoup.com/ (last visited on April 17, 2024).

[62] *See* Mike Brassfield, *This Company Will Pay You $50 This Year Just for Downloading Its Free App* (May 31, 2019), https://www.thepennyhoarder.com/make-money/nielsen-panel/ (last visited on April 17, 2024).

[63] *See Medical I.D. Theft*, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last visited on April 17, 2024).

153. The fraudulent activity resulting from the Data Breach may not come to light for years.

154. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

155. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to more than eight hundred thousand individuals' detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

156. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

157. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

158. Such fraud may go undetected until debt collection calls commence months or even years later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

159. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

160. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss Of Benefit Of The Bargain

161. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for the provision of healthcare services, Plaintiff and other reasonable patients understood and expected that they were, in part, paying for the healthcare services and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received healthcare services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Samuel Tsou's Experience

162. Plaintiff Samuel Tsou ("Plaintiff Tsou") is, and at all relevant times has been, a resident and citizen of El Monte, California.

163. Plaintiff Tsou was diagnosed with cancer in 2021 and has been a patient with Defendant for several years.

164. As a condition of obtaining healthcare services from Defendant, Plaintiff Tsou was required to provide his Private Information to Defendant, including, but not limited to, his name, date of birth, contact information, health insurance information, Social Security number, and other sensitive information.

165. At the time of the Data Breach—September 19, 2023, through October 12, 2023—Defendant maintained Plaintiff Tsou's Private Information in its system.

166. Plaintiff Tsou first became aware of the Data Breach upon receiving the

Notice Letter directly from Defendant, by U.S. mail, dated April 2, 2024. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties.

167. As a result of the Data Breach, and in accordance with the instructions from Defendant's Notice Letter advising Plaintiff Tsou to "remain vigilant to protect against potential fraud and identity theft by reviewing your account statements, monitoring your credit reports, and notifying your financial institutions of any potential suspicious activity[,]"[64] Plaintiff Tsou took reasonable steps to mitigate the detriment of the breach. His remedial measures included researching the Data Breach, enrolling in credit monitoring and identity theft protection services, scrutinizing his credit report, and vigilantly monitoring his financial accounts for signs of fraudulent activity, which may take years to surface.

168. Plaintiff Tsou devoted substantial time to addressing the consequences of the Data Breach—a significant investment of time that he would have otherwise allocated to other pursuits, such as work or leisure. This time is irretrievably lost and cannot be recovered.

169. Plaintiff Tsou exercises great caution with his sensitive Private Information, securely storing any documents that contain such data in a well-protected location. He has consistently refrained from transmitting unencrypted sensitive Private Information over the internet or any other unsecured channel. Had Plaintiff Tsou known of Defendant's inadequate data security policies, he would not have entrusted his Private Information to Defendant.

170. Plaintiff Tsou suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate

[64] *See* Footnote No. 53.

the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

171. Plaintiff Tsou additionally suffered an actual injury in the form of damage to his credit score. Based on information and belief, the damage to his credit score was caused by the Data Breach.

172. Plaintiff Tsou also suffered a large increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. Plaintiff Tsou reasonably believes that misuse of his PII occurred because cybercriminals are able to easily locate various pieces of information about an affected individual with the Private Information stolen in the Data Breach.

173. The Data Breach has caused Plaintiff Tsou to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully provided Plaintiff with critical details regarding the Data Breach.

174. Had Plaintiff Tsou been aware that Defendant would fail to adequately protect his PII, he would not have granted Defendant access to his Private Information.

175. Since Plaintiff Tsou became aware of the Data Breach on or about April 2, 2024, he has been spending approximately 10 hours per week on proactive measures to remediate the repercussions of the Data Breach. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

176. As a result of the Data Breach, Plaintiff Tsou is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

177. Plaintiff Tsou has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

178. Plaintiff brings this nationwide class action on behalf of himself and behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

179. The Classes that Plaintiff seeks to represent is defined as follows:

Nationwide Class
All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in April 2024 (the "Nationwide Class").

California Subclass
All individuals residing in the state of California whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in April 2024 (the "California Subclass").

180. The Nationwide Class and the California Subclass shall be collectively referred to herein as the "Class" or "Classes" unless otherwise specified.

181. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

182. Plaintiff reserves the right to amend the definitions of the Class and/or California Subclass or add a Class or Subclass if further information and discovery

indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

183. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. According to the breach report submitted to the Office of the Maine Attorney General, at least 827,149 Class Members were impacted in the Data Breach.[65] The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

184. Common questions of law and fact exist as to all Class Members and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions that may affect individual Class Members, are the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;
b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
c. Whether Defendant had respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;
d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;
e. Whether and when Defendant actually learned of the Data Breach;
f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

[65] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/1bb296e2-ea79-438c-b357-28ef738a0bf6.shtml (last visited on April 18, 2024).

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

185. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

186. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

187. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that

would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

188. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

189. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

190. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

191. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

192. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

193. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

194. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;
b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard patient Private Information; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

195. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

196. Defendant requires its patients, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing its healthcare services.

197. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

198. Plaintiff and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

199. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

200. By voluntarily undertaking and assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could

detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

201. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

202. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

203. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiff or Class Members of the Data Breach until April 2, 2024, despite, upon information and belief, Defendant knowing shortly after October 13, 2023, that unauthorized persons had accessed and acquired the private, protected, Private Information of Plaintiff and the Class.

204. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks adequately protected the Private Information.

205. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted

Defendant with their confidential Private Information, a necessary part of being patients with Defendant.

206. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

207. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

208. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information that was no longer required to retain pursuant to regulations.

209. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

210. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

211. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations, and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

212. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

213. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act and HIPAA were intended to protect, and the type of harm resulting from the Data Breach was the type of harm the statutes intended to guard against.

214. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

215. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

216. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

217. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members.

Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

218. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

219. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems or transmitted through third party systems.

220. It was foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

221. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

222. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

223. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

224. Defendant admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

225. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

226. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. Their Private Information was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

227. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer various injuries, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data, evidenced by the increase in spam calls, texts, and/or emails; (viii) Plaintiff's and Class Members' Private Information being disseminated on the dark web; (ix) a significant decrease in Plaintiff's credit score; (x) statutory damages; (xi) nominal damages; and (xii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

228. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to

further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

229. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

230. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach Of Implied Contract
(On Behalf of Plaintiff and the Class)

231. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

232. Plaintiff and Class Members were required deliver their Private Information to Defendant as part of the process of obtaining healthcare services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for healthcare services.

233. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

234. Defendant accepted possession of Plaintiff'' and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

235. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

236. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including HIPAA and FTC guidelines on data security) and were consistent with industry standards.

237. The agreement for Plaintiff and Class Members to provide Private Information to Defendant implicitly included an obligation for Defendant to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

238. The mutual understanding and intent of Plaintiff and Class Members, on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

239. On information and belief, at all relevant times, Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

240. Upon information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

241. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

242. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

243. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

244. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

245. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

246. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their Private Information , by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that Private Information was compromised as a result of the Data Breach.

247. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members, and continued acceptance of PII and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

248. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer various injuries, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting

to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data, evidenced by the increase in spam calls, texts, and/or emails; (viii) Plaintiff's and Class Members' Private Information being disseminated on the dark web; (ix) a significant decrease in Plaintiff's credit score; (x) statutory damages; (xi) nominal damages; and (xii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

249. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

250. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

251. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

252. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

253. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid Defendant and/or its affiliates for healthcare services and, in so doing, also provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the healthcare services that

were the subject of the transaction and should have had their Private Information protected with adequate data security.

254. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

255. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

256. Defendant acquired the Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

257. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information to Defendant or obtained healthcare services at Defendant.

258. Plaintiff and Class Members have no adequate remedy at law.

259. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

260. As a direct and proximate result of Defendant's unreasonable and inadequate data security practices, Plaintiff and the Class have suffered and will suffer various injuries, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data, evidenced by the increase in spam calls, texts,

and/or emails; (viii) Plaintiff's and Class Members' Private Information being disseminated on the dark web; (ix) a significant decrease in Plaintiff's credit score; (x) statutory damages; (xi) nominal damages; and (xii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

261. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

262. Plaintiff and Class Members may not have an adequate remedy at law against Defendant. Accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §17200 *et seq.* (On Behalf of Plaintiff and the Class)

263. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

264. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

265. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

266. Defendant's "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' Private

Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), HIPAA, California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

267. Defendant has engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45, and California common law.

268. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private

Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA.

269. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

270. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members' were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information.

271. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

272. Plaintiff and Class Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

273. By deceptively storing, collecting, and disclosing their Private Information, Defendant has taken money or property from Plaintiff and Class Members.

274. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

275. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT V
Violation of the California Customer Records Act,
Cal. Civ. Code §§ 1798.80 *et seq.*
(On Behalf of Plaintiff and the California Subclass)

276. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein, and brings this claim on behalf of himself and the California Subclass.

277. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

278. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

279. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

280. Plaintiff and the California Subclass Members are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant for the purpose of obtaining a product and/or service from Defendant.

281. The Private Information of Plaintiff and the California Subclass Members at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the

identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

282. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and California Subclass Members' Private Information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information of Plaintiff and the California Subclass Members. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information of Plaintiff and the California Subclass Members from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and the California Subclass Members' nonencrypted and nonredacted Private Information to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

283. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the Private Information of Plaintiff and the California Subclass Members included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the Private Information of Plaintiff and the California Subclass Members by the cyber attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

284. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the California Subclass Members were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the California Subclass Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

285. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

286. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

   i. the date of the breach,

   ii. the estimated date of the breach, or

   iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

287. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and California Subclass Members. On information and belief, to date, Defendant has not sent written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all California Subclass Members. Not all California Subclass Members have been notified of the breach; members could have taken action to protect their PII, but were unable to do so because they were not timely notified of the breach.

288. On information and belief, many California Subclass Members affected by the Data Breach have not received any notice at all from Defendant in violation of Section 1798.82(d).

289. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and

California Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

290. As a direct consequence of the actions as identified above, Plaintiff and California Subclass Members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

COUNT VI
Violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

291. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein, and brings this claim on behalf of himself and the California Subclass.

292. Defendant is "a provider of health care," as defined in Cal. Civ. Code §56.05(m), and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

293. At all relevant times, Defendant was a health care provider because they had the "purpose of maintaining medical information to make the information available to the individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manager his or her information, or for the diagnosis or treatment of the individual."

294. As a provider of health care or a contractor, Defendant is required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated, and/or released without the patient's authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

295. As a provider of health care or a contractor, Defendant is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

296. Defendant is a person/entity licensed under California under California's Business and Professions Code, Division 2. See Cal. Bus. Prof. Code § 4000, *et seq*.

297. Plaintiff and California Subclass Members are "patients" as defined in CMIA, Cal. Civ. Code §56.05(k) ("'Patient' means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains.") Furthermore, Plaintiff and California Subclass Members, as patients and customers of Defendant, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network, and were patients on or before the date of the Data Breach.

298. Defendant negligently created, maintained, preserved, stored, and then exposed Plaintiff's and California Subclass Members' individually identifiable "medical information," within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiff's and California Subclass Members' names, addresses, medical information, and health insurance information, that alone or in combination with other publicly available information, reveals their identities. Specifically, Defendant knowingly allowed and affirmatively acted in a manner that allowed unauthorized parties to access, exfiltrate, and actually view Plaintiff's and California Subclass Members'

confidential Private Information.

299. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and California Subclass Members to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and California Subclass Members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

300. Defendant also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential personal medical information.

301. Plaintiff's and California Subclass Members' medical information was accessed and actually viewed by hackers in the Data Breach.

302. Plaintiff's and California Subclass Members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

303. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A). As a direct and proximate result of Defendant's above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the California Subclass Members have suffered (and will continue to suffer) economic damages and other injury and actual harms including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs

associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's and California Subclass Members' Private Information being disseminated on the dark web; (ix) a significant decrease in Plaintiff's credit score; (x) statutory damages; (xi) nominal damages; and (xii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

304. As a direct and proximate result of Defendant's wrongful actions, inaction, omission, and want of ordinary care that directly and proximately caused the release of Plaintiff's and California Subclass Members' Private Information, Plaintiff and California Subclass Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff's and California Subclass Members' written authorization.

305. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and California Subclass Members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA.

306. Plaintiff and the California Subclass Members were injured and have suffered damages, as described above, from Defendant's illegal and unauthorized disclosure and negligent release of their medical information in violation of Cal. Civ. Code § 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

///

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grants the following:

A. For an Order certifying the Classes, and appointing Plaintiff and his Counsel to represent the Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiff's and Class Members' respective lifetimes;

///

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal

identifying information of Plaintiff and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect himself;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xviii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: April 19, 2024

Respectfully Submitted,

By: /s/ M. Anderson *Berry*

M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
Brandon P. Jack (SBN 325584)
Michelle Zhu (SBN 347741)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
12100 Wilshire Boulevard, Suite 800
Los Angeles, CA 90025
Tel: (747) 777-7748
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com
mzhu@justice4you.com

Attorneys for Plaintiff and the Proposed Class